



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,181	02/28/2002	Akiko Kuwayama	0378-0386P	4914
2292	7590	01/24/2006		
BIRCH STEWART KOLASCH & BIRCH PO BOX 747 FALLS CHURCH, VA 22040-0747				
			EXAMINER DANIELS, ANTHONY J	
			ART UNIT	PAPER NUMBER
			2615	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

Response to Amendment

1. The amendment, filed 11/10/2005, has been entered and made of record. Claims 1-28 are pending in the application.

Response to Arguments

2. Applicant's arguments filed 11/10/2005 have been fully considered but they are not persuasive.

In regard to the arguments on pp. 15-19 entitled § 103 REJECTION – STEINBURG, WASULA, the examiner respectfully disagrees. On p. 16, paragraph 3, Lines 1,2, applicant alleges, “A closer inspection indicates that the profiles [of Wasula] have no identifying relationship whatsoever...”. Applicant further alleges on p. 17, paragraph 1, Lines 3-5, that, “...Wasula is utterly silent regarding any type of identifier, let alone an identifier that is specific to fingerprint data...”. In a first statement of support for these allegations, applicant has asserted that the profiles are merely customized instructions on transferring images from the camera to the external device (p. 17, paragraph 1, Lines 1,2). In a second statement of support, applicant has asserted that a user has access to multiple customized profiles (p. 17, paragraph 2, Lines 1-3). In regard to the first statement of support, the fact that these customized profiles contain transferring instructions does not imply that they do not identify a user. In evidence, examiner points to the Figure 3A of Wasula where the profile name is JOHN HOME USE. Indeed, it cannot be disputed that that the profile name can be interpreted as an identifier particular to fingerprint data, when the identifier identifies a particular person with fingerprint data.

Art Unit: 2615

Furthermore, for the most part, the profile name is used by multiple users to differentiate their profiles from other users' profiles on the camera. In regard to the second statement of support, it seems as if applicant has misunderstood the teaching of Wasula on paragraph [0029], Lines 17-22, the applicant seems to think this citation means that the user can access others' profiles. This citation merely states that users can create multiple profiles for themselves. Furthermore, Wasula discloses that access can be denied to unauthorized users by employing a password for each profile ([0043]).

In regard to applicant's arguments on p. 13, entitled § 102 REJECTION – STEINBERG, the examiner respectfully disagrees. Independent claim 9 now recites, in part “automatically initiating a registering of the inputted fingerprint data ... in case no fingerprint data is registered...”. Applicant has stated that, “...the examiner admits that such a feature is not taught or suggested in Steinberg...” (p. 1, paragraph 5, Lines 1,2). It is respectfully submitted that the examiner has never stated that Steinberg does not teach this feature. The examiner has only said that registering is initiated by a user input, but this is not the only form of initiation. In particular, the accepting of the password by the camera can be viewed as the actual initiation, because the accepting of the password precedes the placing of the finger of the shutter button.

In regard to applicant's arguments on p. 14 paragraphs 2-4, of § 102 REJECTION – STEINBERG, the examiner respectfully disagrees. The “first time ever” language still leaves the claim broad enough to be read on by Steinberg, because the claim does not specify who is using the camera is for the first time ever. Consequently, it follows that the accepting of the password and the registration of fingerprint data is an indication that the person using the camera is using it for a first time ever.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 9,13,17-19,23,26 is rejected under 35 U.S.C. 102(e) as being anticipated by Steinberg et al. (US 6,433,818).

As to claim 9, Steinberg et al. teaches a method of personal identification for use in a digital camera (Col. 2, Lines 3-6), comprising the steps of: inputting fingerprint data to the digital camera (Figure 10, Figure 12; Col. 6, Lines 5-10); checking if the inputted fingerprint data is identical with fingerprint data registered with a fingerprint register of the digital camera (Col. 6, Lines 10-15); and automatically initiating a registering of the inputted fingerprint data having a corresponding identifier with the fingerprint register in case no fingerprint data is registered with the fingerprint register (*This action is inherent in the system of Steinberg et al., in that a database would have to be created in order for the camera to operate as explained. See response to arguments section, paragraph 2.*).

As to claim 13, Steinberg et al. teaches a method for allowing access to a digital camera, comprising: receiving fingerprint data of a user of the digital camera (Col. 6, Lines 5-10); determining if the digital camera is being used for a first time ever (*If a user enters the password and the password is accepted, this is an indication that the user is using the camera for the first time ever with the correct password. If he/she wishes to enter their fingerprint data, then they have not used the camera before. The user will input his/her fingerprint data into the database, so that he/she can have access to the camera.*); and registering the fingerprint data of the user

Art Unit: 2615

when it is determined that the digital camera is being used for the first time ever (Col. 6, Lines 5-10; *{The acceptance of the password is the signal that the user has not used the camera before and wishes to enter his/her biometric data into the database.}*).

As to claim 17, Steinberg et al. teaches the method of claim 13, further comprising: determining whether the user is a registered user when it is determined that the digital camera is not being used for the first time ever (Col. 5, Lines 47-50; *{Examiner interprets the camera not being used for the first time ever as not accepting the password, a prospective user will try to take a picture not enter a password and the judgment is made by the camera from there whether he/she is an authorized user.}*); and disallowing access when it is determined that the user is not a registered user (Col. 5, Lines 48-50).

As to claim 18, Steinberg et al. teaches the method of claim 17, wherein the step of determining whether the user is a registered user comprises: comparing the fingerprint data of the user with one or more fingerprint data of registered users of the digital camera; determining that the user is registered if the fingerprint data of the user matches with any of the one or more fingerprint data of registered users; and determining that the user is not registered if the fingerprint data of the user matches with none of the one or more fingerprint data of registered users (Col. 5, Lines 43-52).

As to claim 19, Steinberg et al. teaches the method of claim 17, further comprising: receiving an instruction (*The instruction is to take an image.*) from the user when it is determined that the user is a registered user (Col. 5, Lines 50-52); and registering a new user to the digital camera when the received instruction specifies registering the new user (Col. 5, Lines 55-67; Col. 6, Lines 1-15).

As to claim 23, Steinberg et al. teaches the method of claim 19, further comprising: determining whether the registered user is authorized to issue the received instruction when the received instruction does not specify registering the new user; and executing the received instruction when it is determined that the registered user is authorized to issue the received instruction (Col. 5, Lines 43-52).

As to claim 26, Steinberg et al. teaches the method of claim 13, further comprising: receiving an instruction (Col. 5, Lines 40-47; *{The pressing of the shutter button.}*) from the user when it is determined that the digital camera is not being used for the first time ever (Col. 5, Lines 47-50; *{Examiner interprets the camera not being used for the first time ever as not accepting the password, a prospective user will try to take a picture not enter a password and the judgment is made by the camera from there whether he/she is an authorized user.}*); determining whether the received instruction is a restricted permission instruction (*This instruction is always restricted permission as opposed to the entering of the password which is not restricted permission. Anyone can try to enter a password.*); and executing the received instruction when it is determined that the received instruction is a restricted permission instruction (Col. 5, Lines 50-52; *{The picture will be taken if the user is authorized.}*).

Claim Rejections - 35 USC § 103

4. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg et al. (see Patent Number above).

As to claim 10, Steinberg et al. teaches the method in accordance with claim 9, further comprising the steps of: comparing the inputted fingerprint data with the fingerprint data

Art Unit: 2615

registered with the fingerprint register in case the fingerprint data is registered with the fingerprint register (see Col. 6, Lines 5-15); and disabling the digital camera in the case no fingerprint data is identified with the inputted fingerprint data (see Col. 5, Lines 43-50).

Although Steinberg et al. does not explicitly teach turning off the power of the digital camera in this embodiment, Steinberg et al. teaches shutting down if a renewal code is not received (Col. 5, Lines 8-11). It would have been obvious to one of ordinary skill in the art to do so, because this provides the same function as disabling the camera; therefore, providing added security to the camera.

5. Claims 1,2,4-8,11,12,24,25,27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg et al. (see Patent Number above) in view of Wasula et al. (US 20020054224).

As to claim 1, Steinberg et al. teaches a digital camera (see Figure 1, digital camera “18”) for picking up a scene with an image sensor (see Figure 10, Figure 2, image acquisition “46”) and forming a frame of image data representative of the scene with a signal processor (see Figure 2, processor “32”), comprising: a fingerprint sensor provided on an exterior of said digital camera for sensing a fingerprint to produce inputted fingerprint data (see Figure 12; Col. 7, Lines 64-67; Col. 8, Lines 1,2; *{The shutter release button is considered part of the fingerprint sensor.}*); a fingerprint register for registering one or more fingerprint data (see Col. 6, Lines 5-15, “...signature database,”); a memory for storing therein frames of image data (see Figure 2, memory “42”; Col. 3, Lines 50-59); a comparison circuit comparing the inputted fingerprint data with the one or more fingerprint data registered with said fingerprint register to produce identified fingerprint data (see Col. 6, Lines 5-15; *{The comparison takes place in the digital*

camera; therefore, a circuit for comparing fingerprint data is inherently in it.}); an authorizer for storing information (see Figure 2, memory “42”; *{The authorizer is being interpreted by examiner as a memory as taught in the specification ([0036])}*); a user interface circuit for inputting an instruction to said digital camera (see Figure 2, keypad “12”; Col. 3, Lines 50-54); and a controller (see Figure 2, processor “32”) for accessing said authorizer (see Figure 2, bus line “44”) and executing an instruction if the instruction is intended to handle a frame of image data **(see Col. 3, Lines 61-63; {The processor executes the instruction of displaying an image on the display. This instruction is intended to handle a frame of image data.})*. The claim differs from Steinberg et al. in that it further requires that a specific identifier is allotted with the fingerprint data, a frame of data is associated with the specific identifier, the authorizer storing the identifier specific to the fingerprint data, and the controller references the identifier stored in said authorizer **(Image data associated with the identifier has already been cited as a difference between claim 1 and Steinberg et al; particularly, when it is said that the claim differs from Steinberg et al. in that it further requires a frame of data associated with the specific identifier.)*.

In the same field of endeavor, Wasula et al. teaches a digital camera (Figure 1, digital camera “10”) for creating profiles for people with fingerprints (Figure 6; [0027], Lines 17-22). The profiles containing images taken by a user and the profiles can be selected from many ([0037], Figure 6). In light of the teaching of Wasula et al., it would have been obvious to one of ordinary skill in the art at the time the invention was made to sort the images taken by each user of the digital camera in Steinberg et al. into the profiles of Wasula et al., because an artisan of ordinary skill in the art would recognize that that this would allow the owner of Steinberg et al.’s

Art Unit: 2615

camera to quickly identify what image data belongs to which renter of the digital camera and to efficiently sort and retrieve files according to photographers.

As to claim 2, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 1, further comprising a shutter release button on which said fingerprint sensor is provided (see Steinberg et al., Figure 12, Col. 7, Lines 64-67; Col. 8, Lines 1-6; *{The shutter release button comprises the transparent layer upon which the fingerprint is sensed which is considered part of the sensor.}*).

As to claim 4, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 1, wherein frames of image data stored in said memory are associated one of the identifiers so that the frames are separately stored in one or more folders prepared in said memory (see Wasula et al., Figure 6, [0037]), said fingerprint register registers therewith folder names for the identifiers, and said authorizer stores therein a folder name (see Wasula et al., [0037], Lines 5-16).

As to claim 5, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 4, wherein the folders in said memory may be grouped under one or more super folders (see Wasula et al., Figure 6, AutoXfer profiles), and the fingerprint data registered with said fingerprint register include folder names of the super folders (*The profiles can be named anything by the user.*).

As to claim 6, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 4, further comprising a record control circuit for storing a folder name specific the fingerprint identified by said comparison circuit (Figure 6), said controller recording,

Art Unit: 2615

response instruction to record a frame of image data formed by said digital camera, the frame into a folder having the folder name ([0037], Lines 17-22).

As to claim 7, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 4, further comprising: a password inputting circuit for inputting a password (see Figure 2, keypad "12"; Col. 5, Lines 55-65); and a password storage storing the password (*It is inherent in the system of Steinberg et al. that the password be stored in the camera, such that there would be something to compare what the user enters.*), said controller outputting, in response instruction to output a folder from said memory to a recording medium, the folder and the password specific to the folder the recording medium (see Figure 2, card slot "16"; *{It is inherent in the system of Steinberg that digital information (password or folder) be transferred to a memory card on basis of instruction.}*). The claim differs from Steinberg et al., as modified by Ohmura, in that it further requires that the password be specific to the folder and required to open the folder.

In the same field of endeavor, Wasula et al. teaches a password that maybe used to gain access to digital images of the customized profile (see [0043]). In light of the teaching of Wasula et al., it would have been obvious to one of ordinary skill in the art at the time the invention was made to prompt a user to enter a key before gaining access to the image folder of Steinberg et al., as modified by Wasula et al., because an artisan of ordinary skill in the art would recognize that such a key would provide added security to the camera while making more difficult for someone without access to obtain it (*Applicant is advised to refer to Steinberg et al., Col. 8, Lines 61-67 in which Steinberg et al. teaches the advantages of a password for gaining private access.*).

As to claim 8, Steinberg et al., as modified by Wasula et al., teaches teaches the digital camera in accordance with claim 1, wherein said authorizer stores no identifier as long as no fingerprint data is identified by said comparison circuit (*It is inherent in the system of Steinberg et al., as modified by Wasula et al., that a folder name would not be stored if a corresponding fingerprint data did not exist.*), said controller executing, in response to an instruction to register new fingerprint data with said fingerprint register, the instruction in the case said authorizer contains a folder name specific to the fingerprint data registered with said register (*It is inherent in the system of Steinberg et al., as modified by Wasula et al., that fingerprint data be registered in the signature database of Steinberg et al., if a folder name for the user exists.*).

As to claim 11, Steinberg et al., as modified by Wasula et al., teaches the method in accordance with claim 10, further comprising the steps of: storing the identifier of the inputted fingerprint data in an authorizer in case the registered fingerprint data is identified with the inputted fingerprint data (*It is inherent in the system of Steinberg et al., as modified by Wasula et al., that identified fingerprint data correspond to a folder name.*); checking if an instruction inputted to the digital camera is intended for a new fingerprint registration; and registering newly inputted fingerprint data with the fingerprint register in the case the instruction inputted is intended for a new fingerprint registration (see Steinberg et al., Figure 8; Col. 5, Lines 55-67; Col. 6, Lines 1-15).

As to claim 12, Steinberg et al., as modified by Wasula et al., teaches the method in accordance with claim 11, further comprising the step of executing the instruction inputted if the instruction is intended to handle a frame of image data associated with an identifier the identifier stored in the authorizer (see Steinberg et al., Col. 3, Lines 61-63; *{The processor executes the*

instruction of displaying an image on the display. This instruction is intended to handle a frame of image data.})).

As to claim **24**, Steinberg et al. teaches the method of claim 23. The claim differs from Steinberg et al. in that it requires that the user is a currently registered user and the step of determining whether the registered user is authorized to issue the received instruction comprises: determining whether the received instruction is intended to handle a frame of image data associated with a storage area corresponding to the currently registered user; and executing the received instruction when it is determined that the received instruction is intended to handle the frame of image data associated with the storage area corresponding to the currently registered user.

In the same field of endeavor, Wasula et al. teaches a digital camera receiving an instruction ([0043]; the checking of a password is the instruction), wherein the instruction is always used to handle a frame of data (Figure 3B). In light of the teaching of Wasula et al., it would have been obvious to one of ordinary skill in the art to include the password of Wasula et al. in the system of Steinberg et al., because this would provide security to the user's customized profile (see Wasula et al., [0043]).

Note for claim 25: The USPTO considers applicant's "or" language to be anticipated by any one of the corresponding choices.

As to claim **25**, Steinberg et al. teaches the method of claim 24, wherein the storage area is considered to be corresponding to the currently registered user if the storage area is the currently registered user's private area or an area associated with a group to which the current registered user belongs (see Wasula et al., [0027], Lines 1-5; [0043]).

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg et al. (see Patent Number above) in view of Wasula et al. (see Patent Number above) and further in view of Kramer (US 20010043728).

As to claim 3, Steinberg et al., as modified by Wasula et al., teaches the digital camera in accordance with claim 1. The claim differs from Steinberg et al., as modified by Wasula et al., in that it further requires that said fingerprint sensor comprise a plurality of electrodes and an insulating film for forming capacitors in combination with a finger, and senses the finger's ridges and troughs according to each amount of electric charge accumulated under the electrodes.

In the same field of endeavor, Kramer et al. teaches a fingerprint sensor that comprises a plurality of electrodes (see [0024], Lines 1-3; *{A third capacitor plate requires that two others exist.}*) and an insulating film (see [0024], Lines 1-5, "...dielectric layer...") for forming capacitors in combination with a finger (see [0024], Lines 1-3), and senses the finger's ridges and troughs according to each amount of electric charge accumulated under the electrodes (see [0024]; *{Capacitors inherently produce an electric charge on the outside of the plates.}*). In light of the teaching of Kramer et al., it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the fingerprint sensor of Steinberg et al. with the finger print sensor of Kramer et al., because an artisan of ordinary skill in the art would recognize that this sensor can operate at a higher frame rate; consequently, the sensor would be small in size and could be fabricated on a single integrated circuit chip (see Kramer et al., [0027]).

As to claim 27, Steinberg et al., as modified by Wasula, teaches the digital camera in accordance with claim 1. Although Steinberg et al., does not teach it explicitly. **Official Notice** is taken that the concept of using volatile memory device in cameras is well known and expected in the art. One of ordinary skill in the art would have been motivated to do this, because volatile memory devices only store information used for an immediate purposes and require less complicated components than the flash memory.

7. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Steinberg et al. (see Patent Number above) in view of Satoh (US 20010002933).

As to claim 28, Steinberg et al. teaches a method of claim 13. The claim differs from Steinberg et al. in that it further requires that the step of determining if the digital camera is being used for a first time ever comprises determining whether there are no registered users.

In the same field of endeavor, Satoh teaches a fingerprint certifying device which allows a fingerprint to be registered when a fingerprint certification is initial ([0029], Lines 8-13). In light of the teaching of Satoh, it would have been obvious to one of ordinary skill in the art to include this step in the aforementioned step of Steinberg et al., because an artisan of ordinary skill would recognize that this would prevent the camera from never being used due to non-existent match (see Satoh, [0029], Lines 10-13; Figure 2).

Allowable Subject Matter

Art Unit: 2615

8. Claims 14-16,20-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: As to claims **14,20**, the prior art does not teach or fairly suggest that the step of registering the fingerprint data of the user when it is determined that the digital camera is being used for the first time ever comprises: acquiring and verifying a password associated with the user; acquiring a second fingerprint data of the user; comparing the first and second fingerprint data of the user; and registering the fingerprint data of the user with a fingerprint register when it is determined that the first and second fingerprint data of the user match., nor that the step of registering the new user to the digital camera when the received instruction specifies registering the new user comprises: receiving a first fingerprint data of the new user; acquiring and verifying a password associated with the new user; acquiring a second fingerprint data of the new user; comparing the first and second fingerprint data of the new user; and registering the fingerprint data of the new user with a fingerprint register when it is determined that the first and second fingerprint data of the new user match.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**


MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anthony J. Daniels whose telephone number is (571) 272-7362. The examiner can normally be reached on 8:00 A.M. - 4:30 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dave Ometz can be reached on (571) 272-7593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/19/2006
AD


DAVID OMETZ
SUPERVISORY PATENT EXAMINER